University of Nottingham
UK | CHINA | MALAYSIA

Lloyd's Register Foundation

Dynamic and Dependent Tree Theory for Fault Tree Analysis (D^2T^2)

John Andrews

March 2024

Next Generation Prediction Methodologies and Tools for System Safety Analysis (NxGen)

Background

- Current Risk Assessment tools include: Fault Tree Analysis, Event Tree Analysis
- The foundations of methodologies for safety critical systems were established in the 1960/70s.
- System technology has advanced and system designs, their operating conditions and maintenance strategies are now significantly different to those of the 1970s.

NxGen Objectives

- Develop a single, generic methodology appropriate to meet the demands of modern industrial systems.
- Upwardly compatible - retain as much of the current methodology features as possible:
    - successfully supported safety assessments to date
    - companies want to retain the safety models they have evolved over time

Industrial Partners

Network Rail

HIGH 1 SPEED

HS2

RSSB

First

NetworkRail High Speed Ltd.

DAE

ATOMS IN THE SERVICE OF THE NATION

igcar

BARC

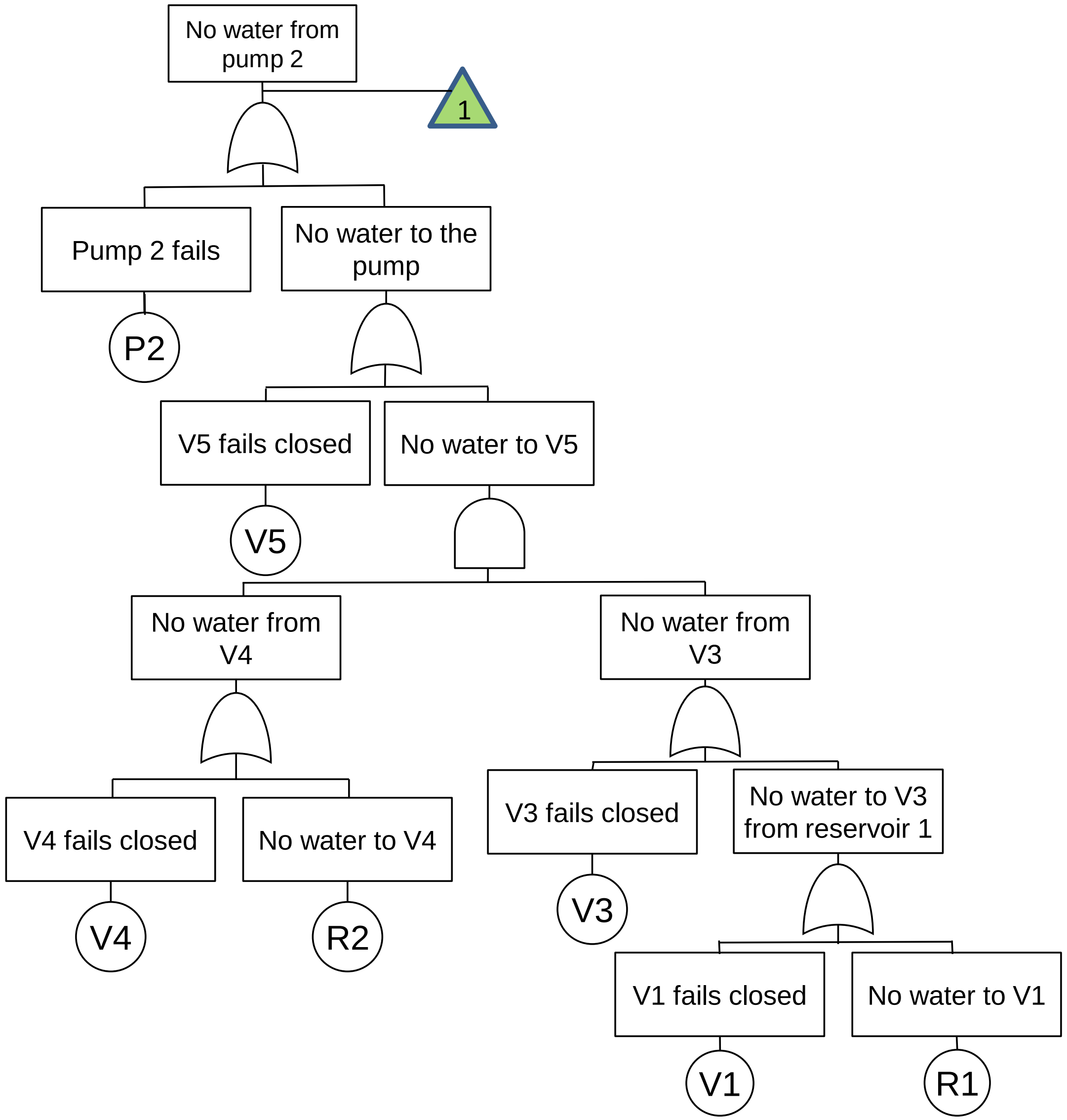
ROLLS ROYCE

BAE SYSTEMS

Lloyd's Register Foundation

Lloyd's Register

Fault Tree Analysis



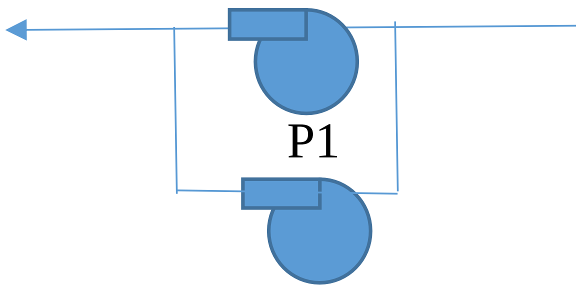
Component failure models

- Limited maintenance process detail
  - No Repair: $Q(t) = F(t) = 1 - e^{-\lambda t}$
  - Revealed: $Q(t) = \frac{\lambda}{\lambda + \nu}\left(1 - e^{-(\lambda+\nu)t}\right)$
  - Unrevealed: $Q_{AV} = \lambda\left(\frac{\theta}{2} + \tau\right)$
- Snap-shot in time

PROJECT AIMS

- Incorporate:
  - non-constant failure rates
  - dependent events
  - dynamic features
  - highly complex maintenance strategies

Standby Systems



Standby System

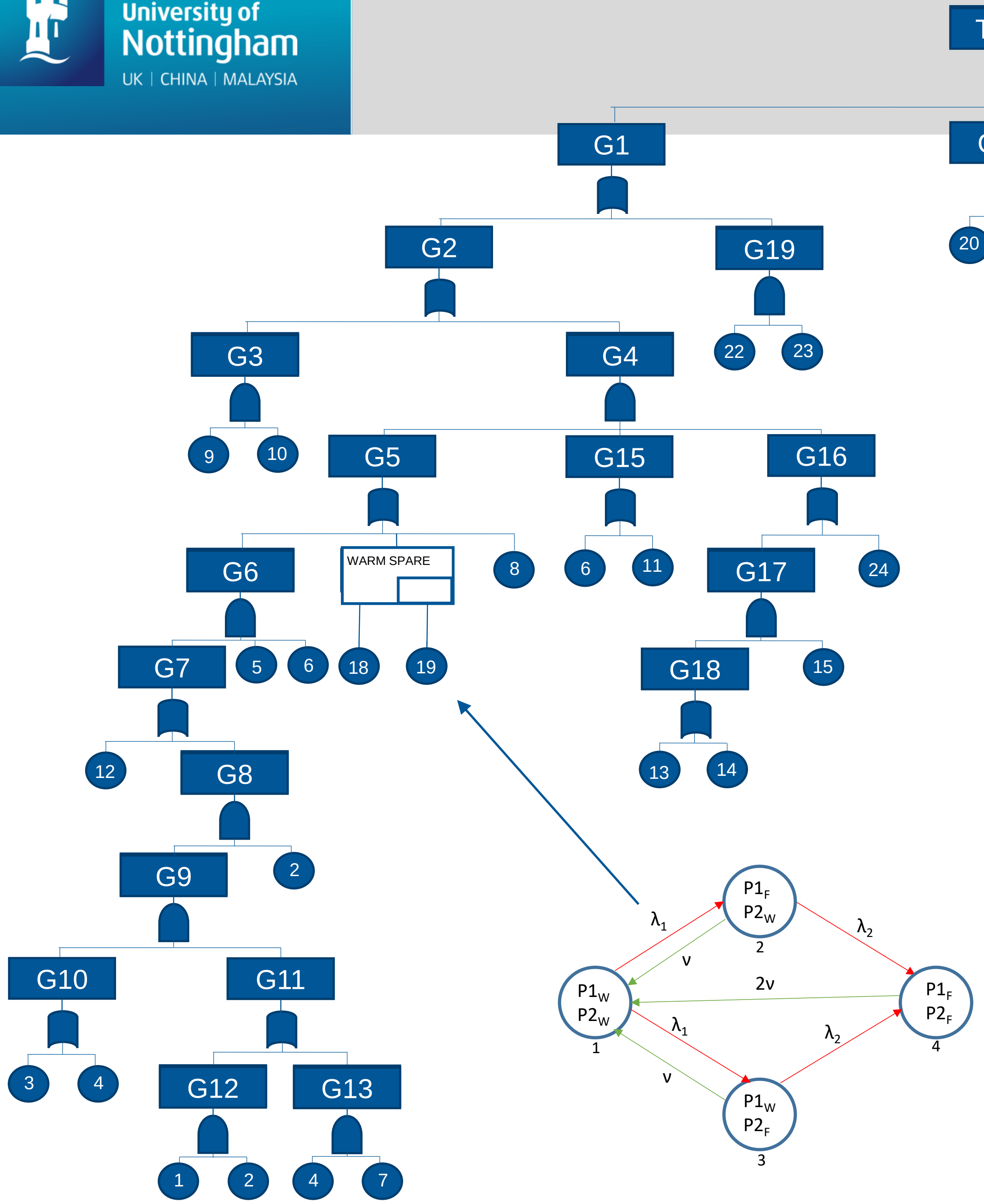
- Pump P1 operational.
- When P1 fails P2 takes over the duty

Hot Standby	Warm Standby	Cold Standby
Both pumps are operational but the fluid is just driven by P1. On failure of P1, the fluid now passes through P2	Pump P2 is not operational in standby. It becomes operational when P1 fails. It can fail in standby but with a lower rate than when operational.	Pump P2 is not operational in standby. It becomes operational when P1 fails. It cannot fail in standby.
P1 & P2 Independent	P1 & P2 Dependent	P1 & P2 Dependent

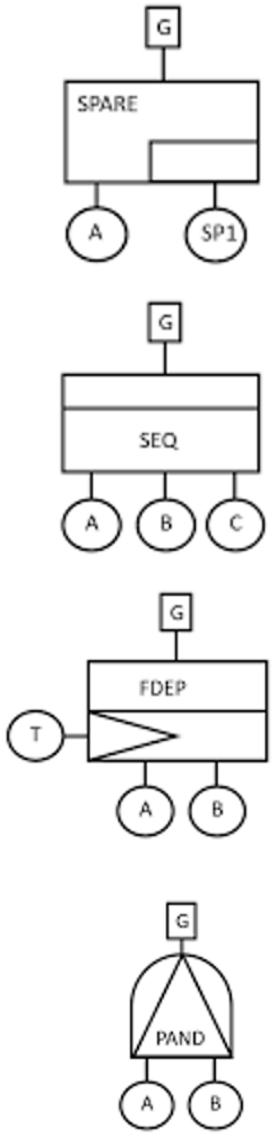
Dependency Examples

Type	Description	Example
Secondary Failure	When one component fails it increases the load on a second component which then experiences an increased failure rate	Two pumps both operational and sharing the load. Each pump has the capability to deliver the full demand should the other pump fail
Opportunistic Maintenance	A component fails which causes a system shutdown or the requires specialist equipment for the repair. The opportunity is taken to do work on a second component which has not failed but is in a degraded state	Components on a circuit board. Components in a sub-sea production module
Common Cause	When one characteristic (eg materials, manufacturing, location, operation, installation maintenance) causes the degraded performance in several components	Incorrect maintenance done on several identical sensors Impact breaks the circuit on cables routed in the same way to different redundant channels
Queueing	Failed components all needing the same maintenance resource are queued. Then repaired in priority order	Limited number of maintenance teams, equipment or spares

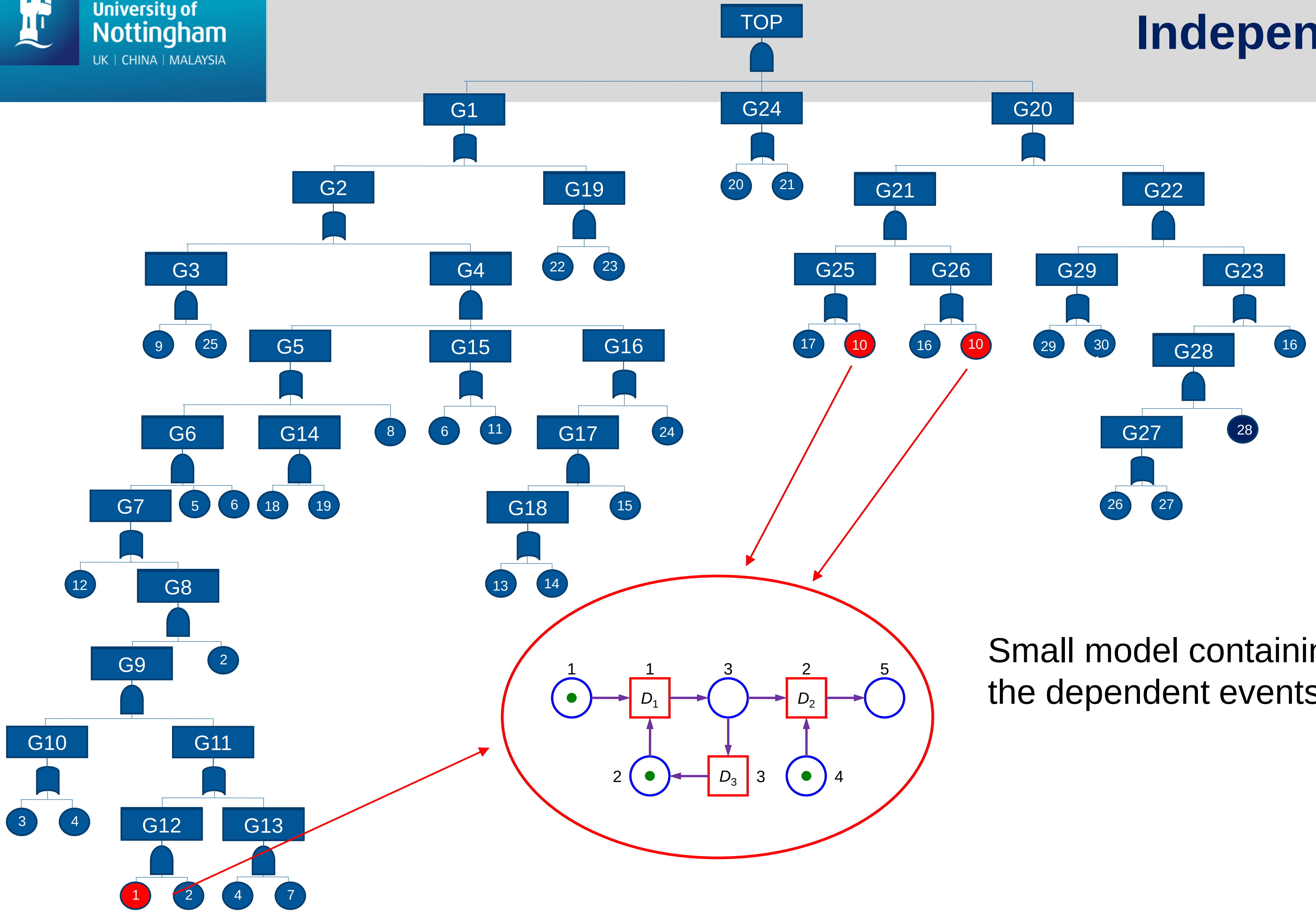
Dynamic Fault Trees



- Difficulties if events 18 or 19 appear elsewhere in the FT



Independent Modules



Maintenance dependency's can affect events which are not geographically close in the FT structure

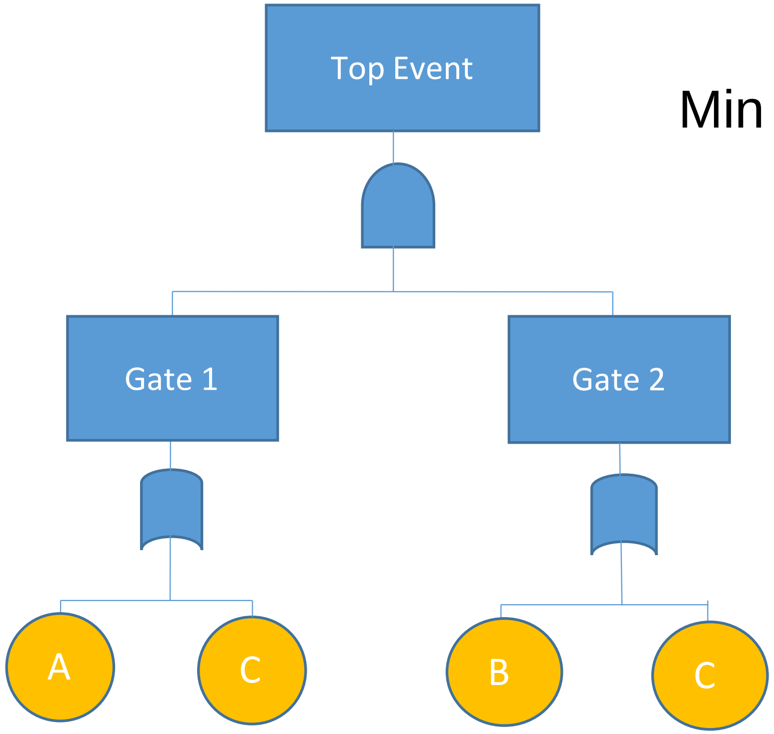
Small model containing only the dependent events

University of Nottingham
UK | CHINA | MALAYSIA

Integration of Fundamental Quantification Methodologies

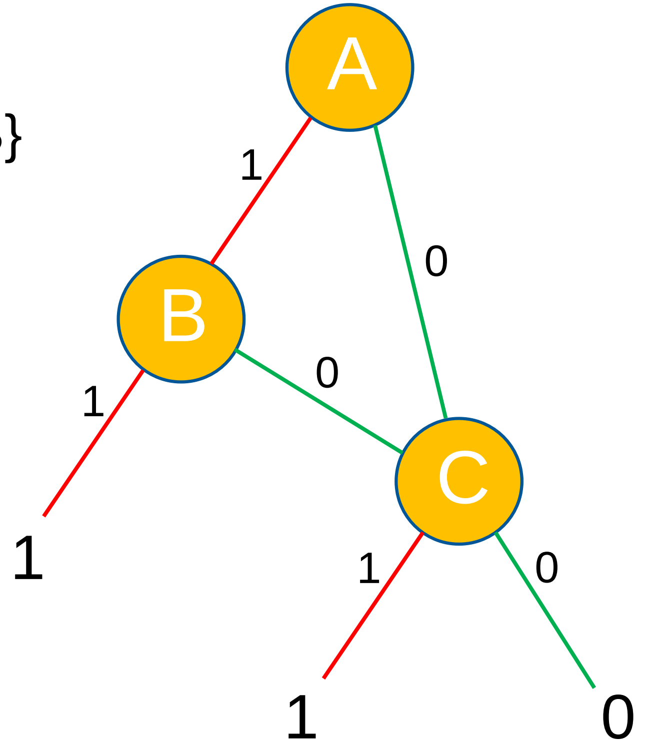
Fault Tree Analysis => Binary Decision Diagrams (BDD)
Petri Nets
Markov Methods

Binary Decision Diagrams – Top Event Probability



Min Cut Sets: {C}, { A, B}

ORDERING A < B < C



\+ OR

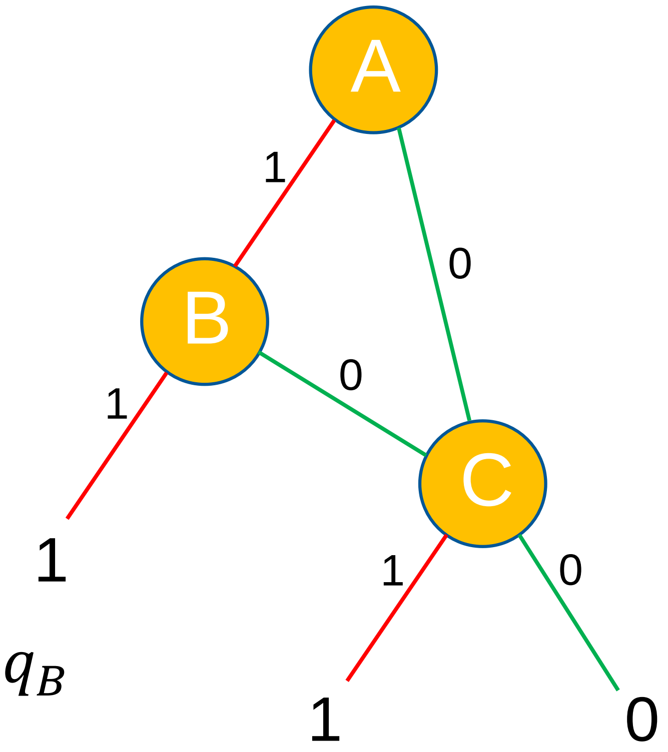
. AND

$$TOP = A.B + C$$

$$TOP = A.B + A.\bar{B}.C + \bar{A}.C$$

$$Q_{SYS} = q_A\, q_B + q_C - q_A\, q_B\, q_C$$

Binary Decision Diagrams – Top Event Probability



$q_A\ q_B$

$q_A(1-q_B)q_C$
$+(1-q_A)\ q_C$

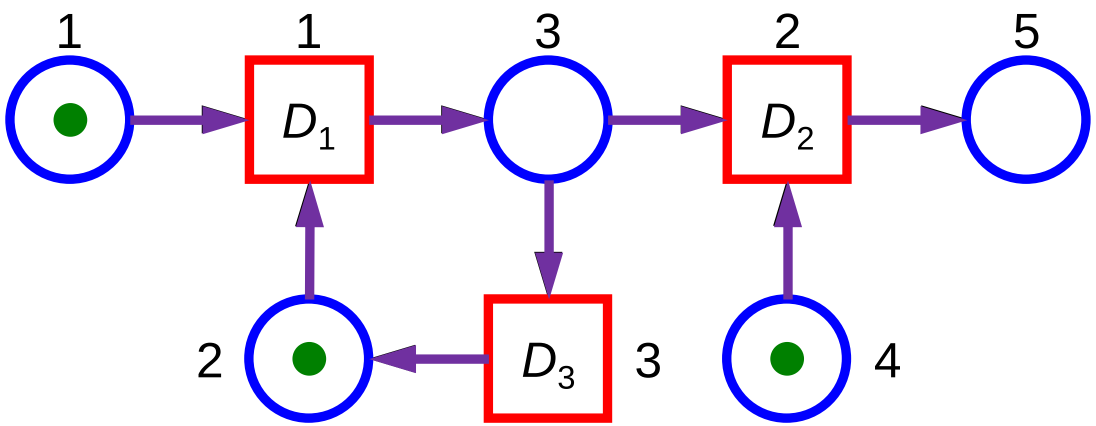
$$Q_{SYS} = q_A\ q_B + q_A(1-q_B)q_C + (1-q_A)\ q_C$$
$$= q_A\ q_B + q_C - q_A\ q_B\ q_C$$

- Exact
- Fast
- Efficient

} No need to derive the Min Cut Sets as an intermediate step

***** Disjoint paths to failure *****

Petri Net Basics and Definitions



Places

Conditions, available resources, counters

Tokens

Mark places
Represent the current status of the system

Transitions

D_j

- Time delay D_j at which transitions occur
- Immediate $D_j = 0$
- Timed $D_j > 0$

Edges

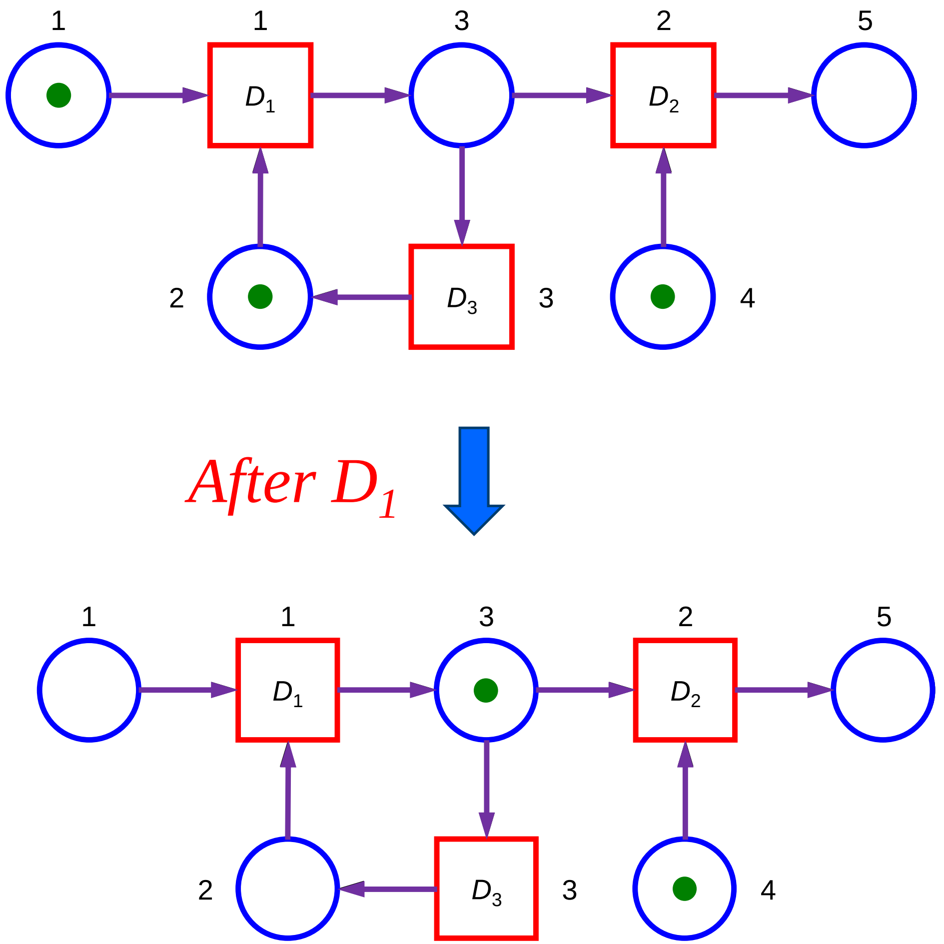
- Input edges
  - place to transition
- Output edges
  - transition to place

Petri Net Modelling

If all input places of a transition are marked by at least one token then this transition is called **enabled**.

After a delay $D \geq 0$ the transition **fires**.

- removes one token from each of its input places
- adds one token to each of its output places.



Petri Net Modelling

Characteristics

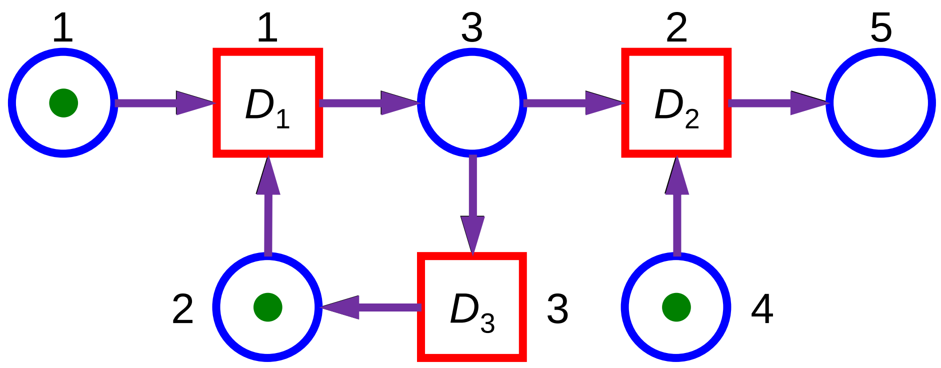
- Any distribution of times to transition
- Capable of modelling very complex maintenance strategies
- Concise structure

Solution

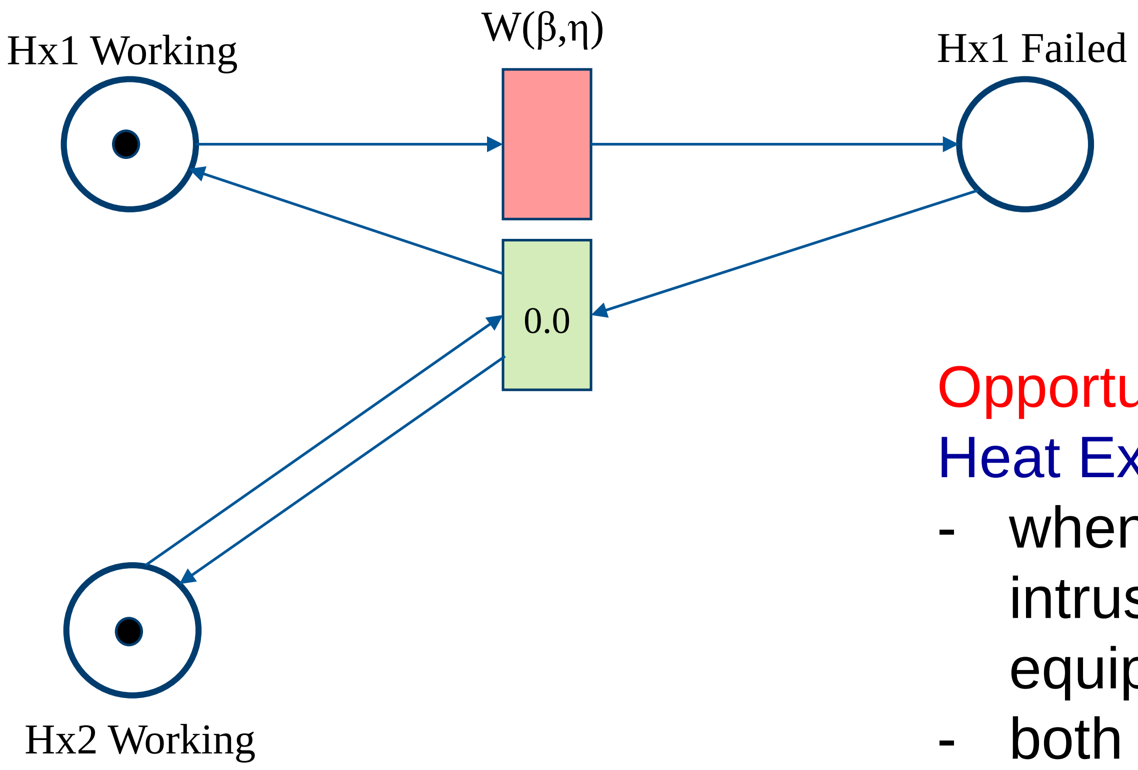
- Monte Carlo Simulation

Outputs

- Produces distributions of:
  - duration in any state
  - no of incidences of entering any state



Dependency Example

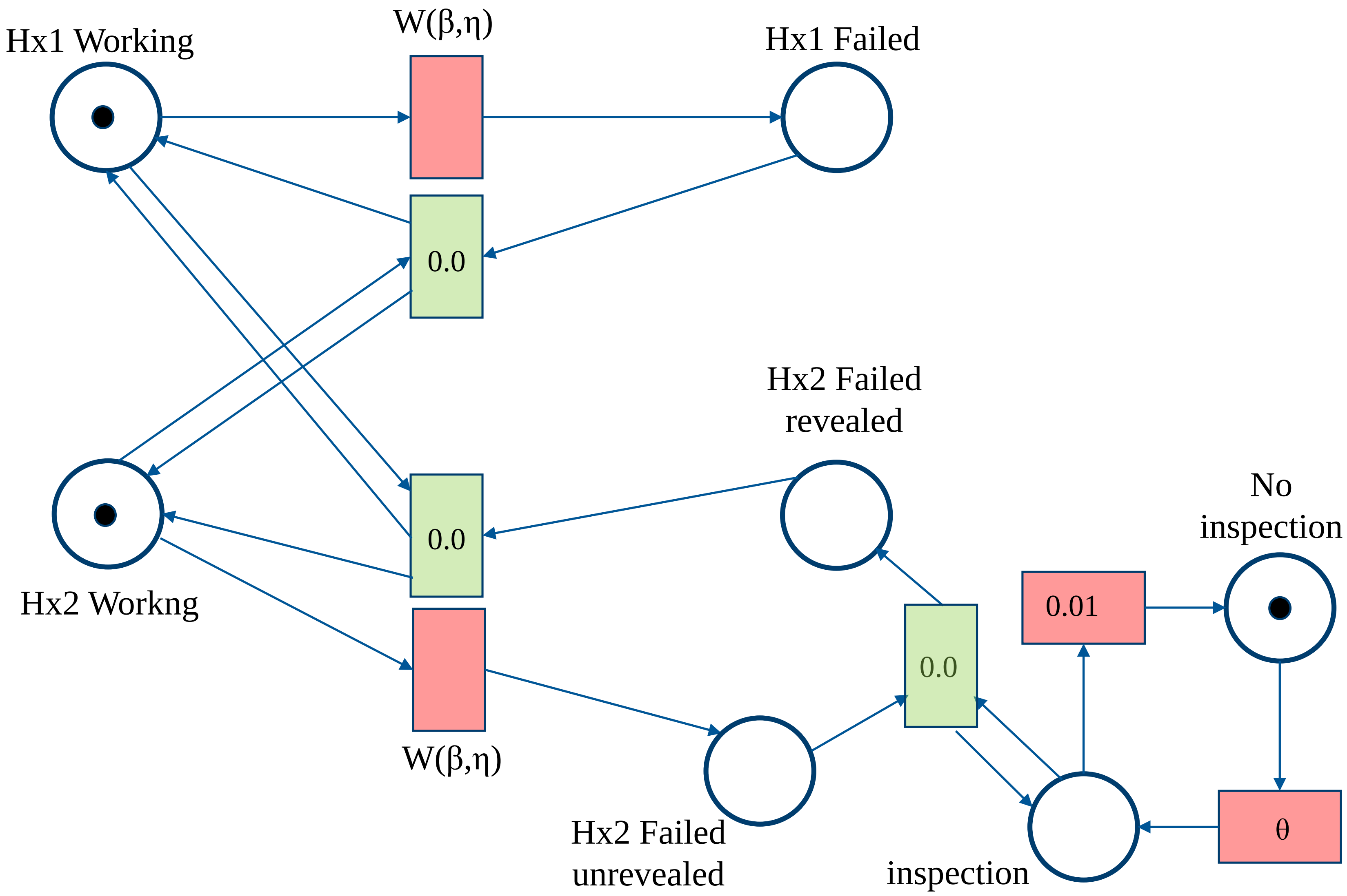


Opportunistic Maintenance Dependency

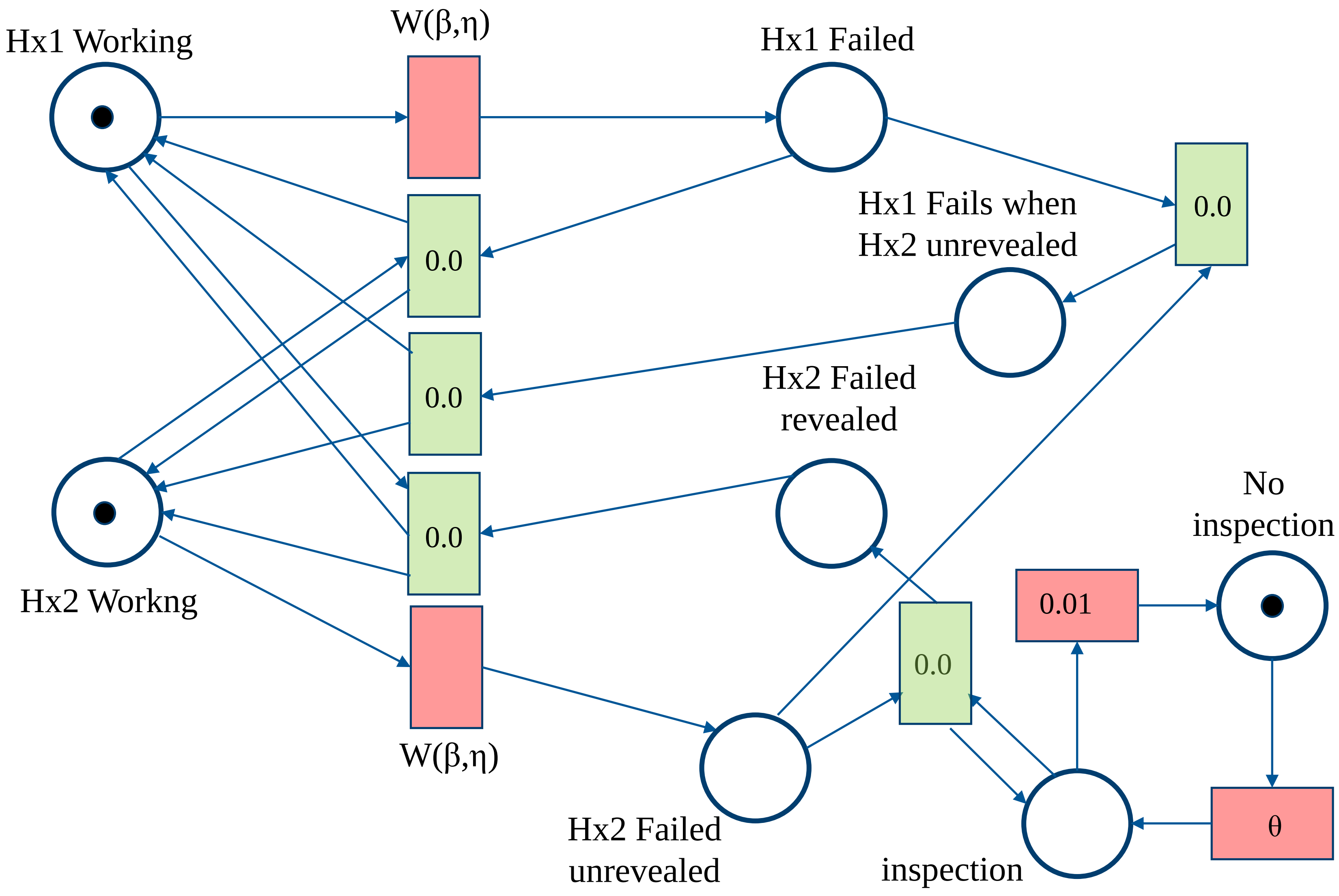
Heat Exchangers Hx1 & Hx2

- when either heat exchanger fails it needs intrusive maintenance requiring specialist equipment
- both are of the same age and operate in the same environment
- the second will fail in the not too distant future
- repair both at the same time
- Hx1 – initiator, Hx2 - enabler

Dependency Example



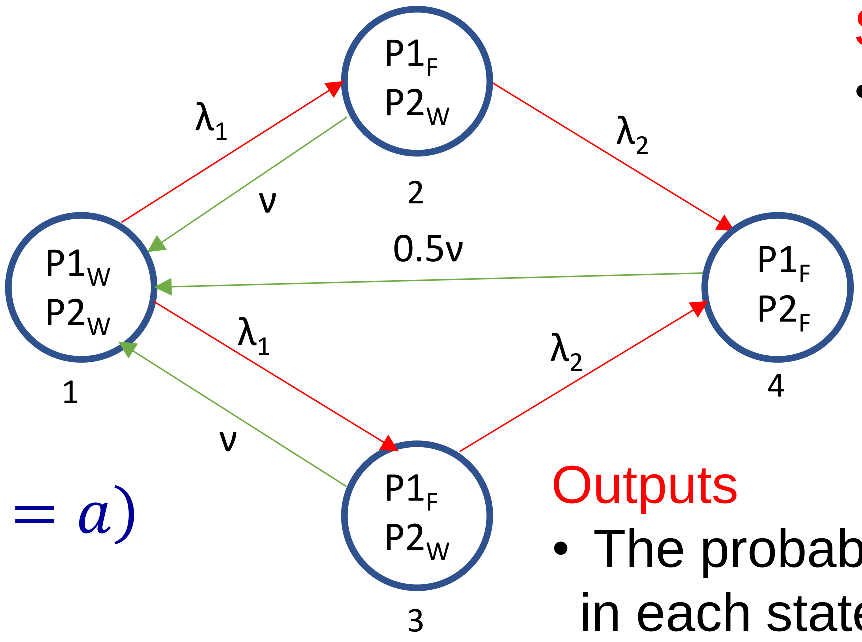
Dependency Example



Markov Analysis

Characteristics

- State – based method
  - States represent the system states
- Memoryless property



Solution

- Numerical Methods

Outputs

- The probability of being in each state at time t

$$P(X_{t+dt} = k \mid X_t = j, X_{t-dt} = i, X_{t-2dt} = h, \ldots, X_0 = a)$$

$$= P(X_{t+dt} = k \mid X_t = j)$$

- Exponential distribution for state residence times (constant transition rates)

$$(\dot{P_1}, \dot{P_2}, \dot{P_3}, \ldots, \dot{P_n}) = (P_1, P_2, P_3, \ldots, P_n)\begin{bmatrix} -\lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & -\lambda_{n,n} \end{bmatrix}$$

University of Nottingham
UK | CHINA | MALAYSIA

Dynamic & Dependent Tree Theory (D^2T^2)

A Fault Tree Analysis Framework

Approach

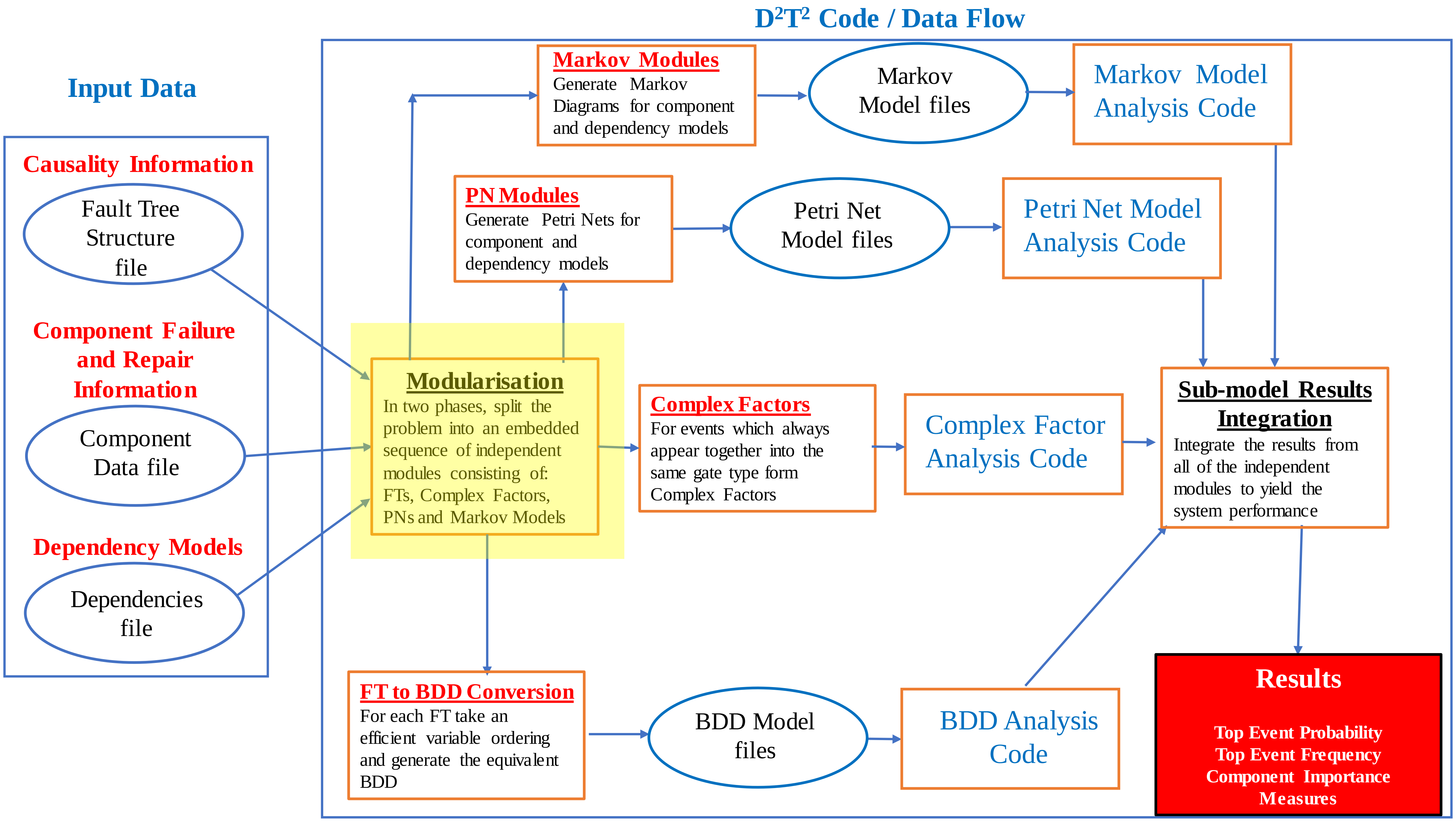
Dependencies

- Model the dependencies and complexities using Petri Nets or Markov models
  - Always use the *simplest dependency model*

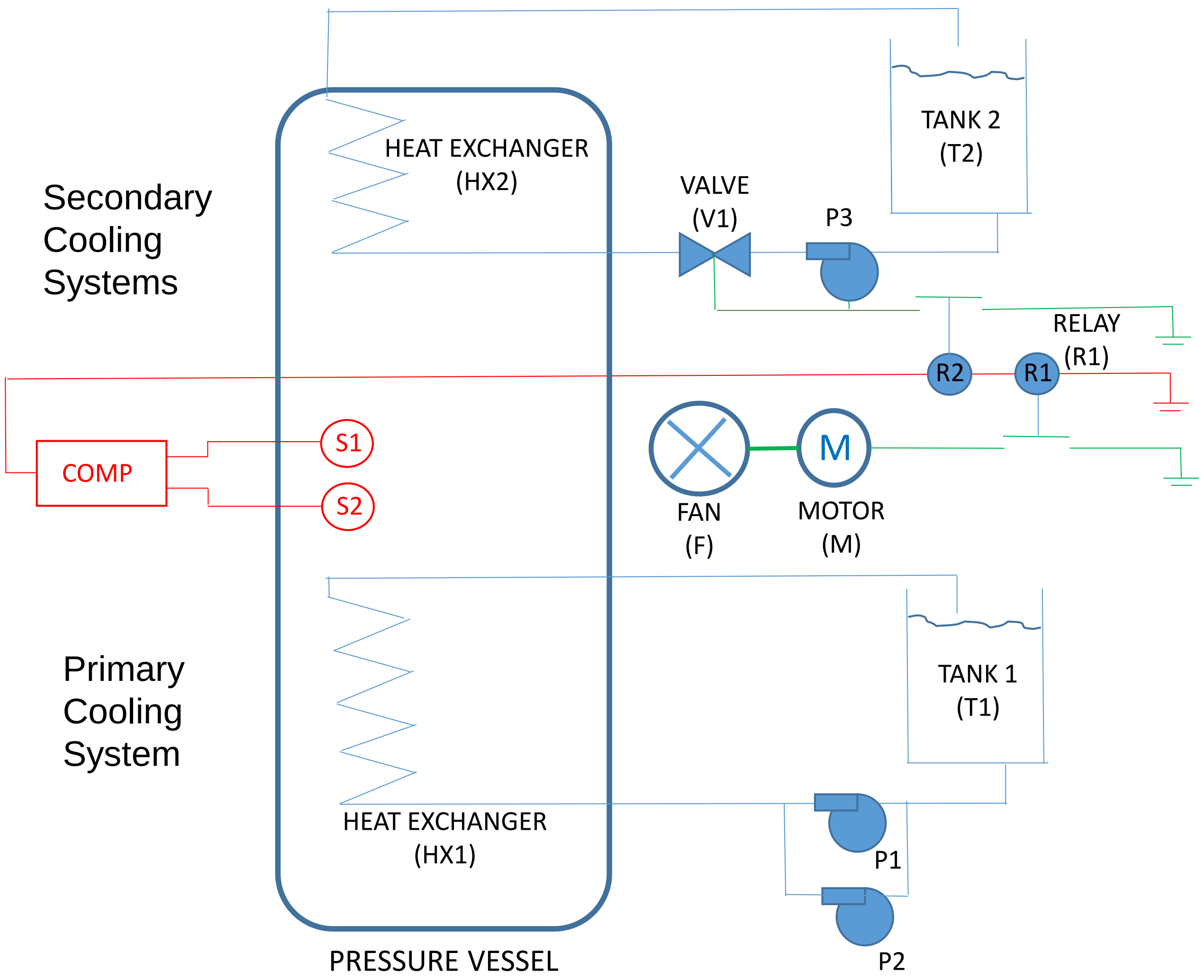
Binary Decision Diagrams

- Dependencies are just required to be considered on each path
- Path numbers can be very high so every effort needs to be made to *minimise the size of the BDD*
  - minimise the fault tree size using an effective modularisation
  - effective variable ordering

Basic Structure of the Code



Plant Cooling System and Features

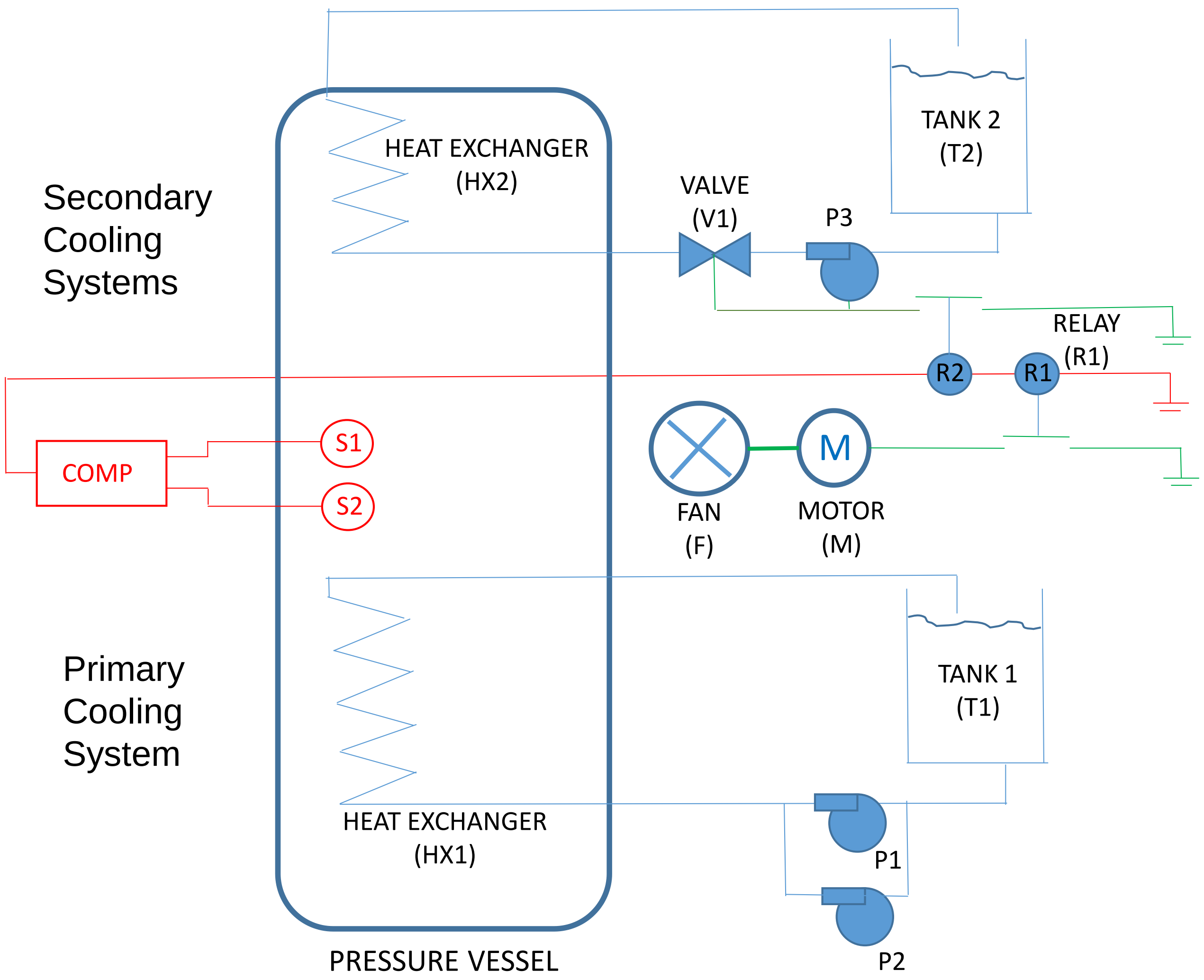


Power supply to all pumps and the valve – B1

Sub-Systems

- Primary Cooling Water System
  - Tank (T1), Pumps (P1,P2), Heat Exchanger (Hx1), Power Supply (B1)
- Detection System
  - Sensors (S1,S2), Computer (Comp)
- Secondary Cooling Water System
  - Tank(T2), Pump (P3), Heat Exchanger (Hx2), Valve (V1), Relay (R2), Power Supply (B1)
- Secondary Cooling Fan System
  - Fan (F), Motor (M), Relay (R1)

Plant Cooling System and Features



Power supply to all pumps and the valve – B1

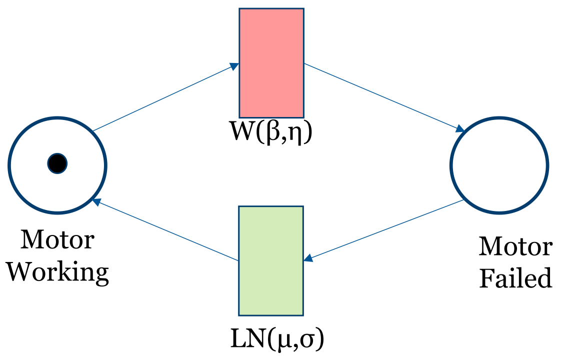
Complex Features

- Non-constant failure / repair rates
  - Motor M - Weibull failure time distribution and a lognormal repair time distribution
- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other
  - Heat Exchangers Hx1 & Hx2 - when one needs replacement – needs specialist equipment and both are replaced
  - Pump P3 - two events P3S and P3R are clearly dependent

Complexity and Dependency Models

- Non-constant failure / repair rates
  - Motor M - Weibull failure time distribution and a lognormal repair time distribution

Failure time distribution - W(β=1.5, η=12,000h)
Repair time distribution - LogN(μ=24h, σ=4.8h)



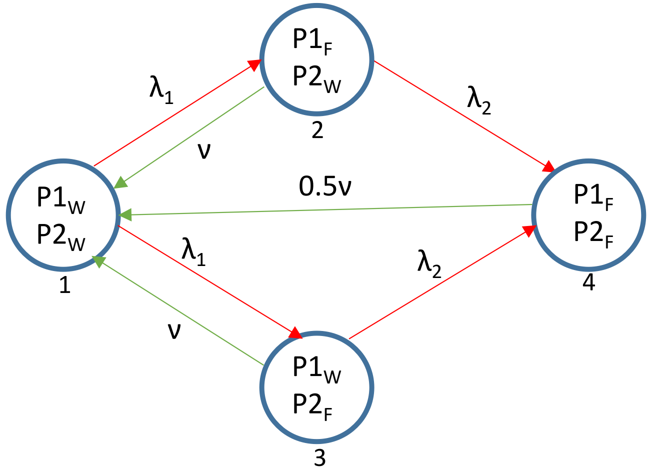
q_{Motor}, failing to operate for 30 hours is 0.005839

- Dependencies
  - Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other

Failure rate $\lambda_1 = 2 \times 10^{-5}$ /h under normal load

$\lambda_2 = 5 \times 10^{-3}$/h under full load

Repair rate ν= 0.041667 (MTTF = 24hrs)



State Number	State	State Probability
1	$P1_W P2_W$	0.99743518
2	$P1_F P2_W$	0.00042747
3	$P1_W P2_F$	0.00042747
4	$P1_F P2_F$	0.00170988

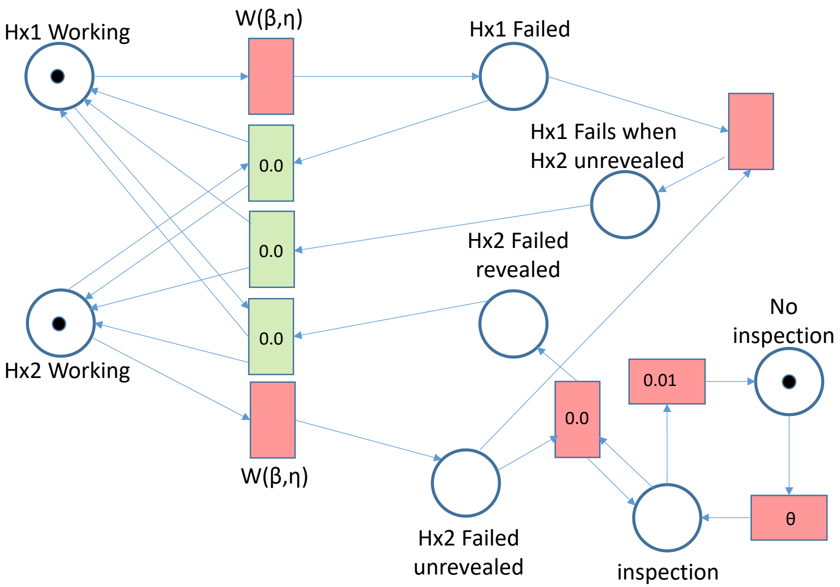
Complexity and Dependency Models

Dependencies

Heat Exchangers Hx1 & Hx2 - when one needs replacement – needs specialist equipment and both are replaced

Failure time = W(β=2.5, η=30,000h)

The system is shut down when the repair is undertaken



$P(Hx1_W, Hx2_W)$=0.98646987828725829

$P(Hx1_W, Hx2_F)$=0.0135301

$P(Hx1_F, Hx2_F)$=0.0

$P(Hx1_F)$=0.0

$P(Hx2_F | Hx1_F)$=0.0

$P(Hx2_F | Hx1_W)$= 0.0135301

$w(Hx1_F$, Hx2_unrevealed)=3.1709792 x 10^{-07} /hour

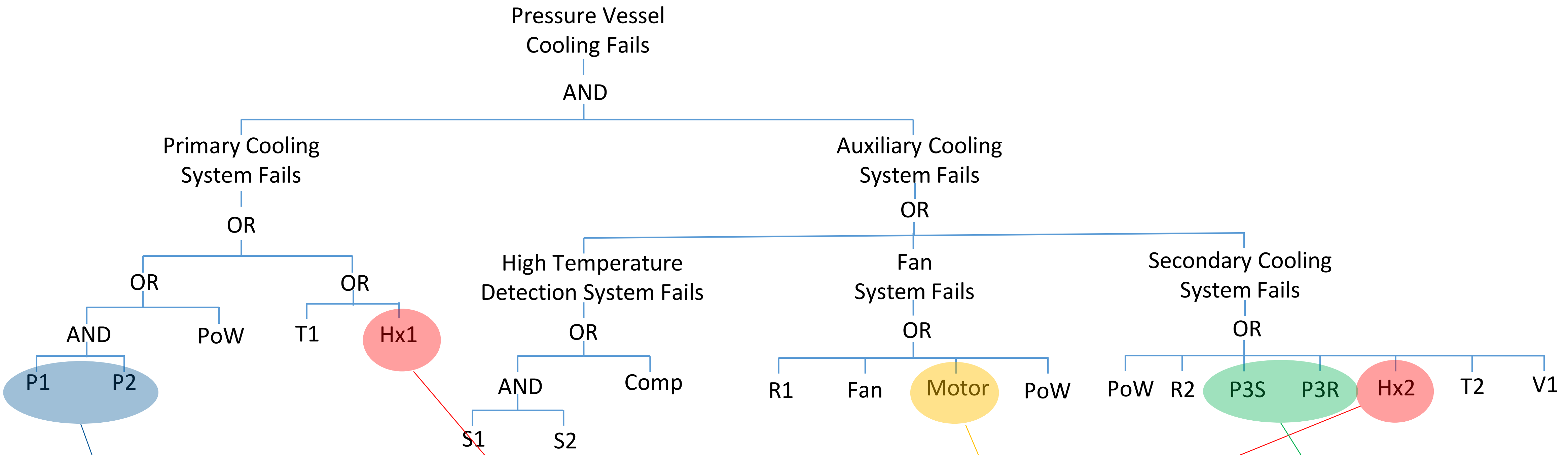
$w(Hx1_F, Hx2_W)$=1.8161063 x 10^{-05} /hour

$w(Hx1_F)$=1.8478161 x 10^{-05} /hour

Pump P3 - two events P3S and P3R are clearly dependent

$$q_{P3} = q_{P3S} + (1.0 - q_{P3S})\lambda_{P3R} t_{period}$$
$$= 0.05 + 0.095 \times 10^{-4} \times 30 \times 24$$
$$= 0.1184$$

Fault Tree Structure and Dependent Events



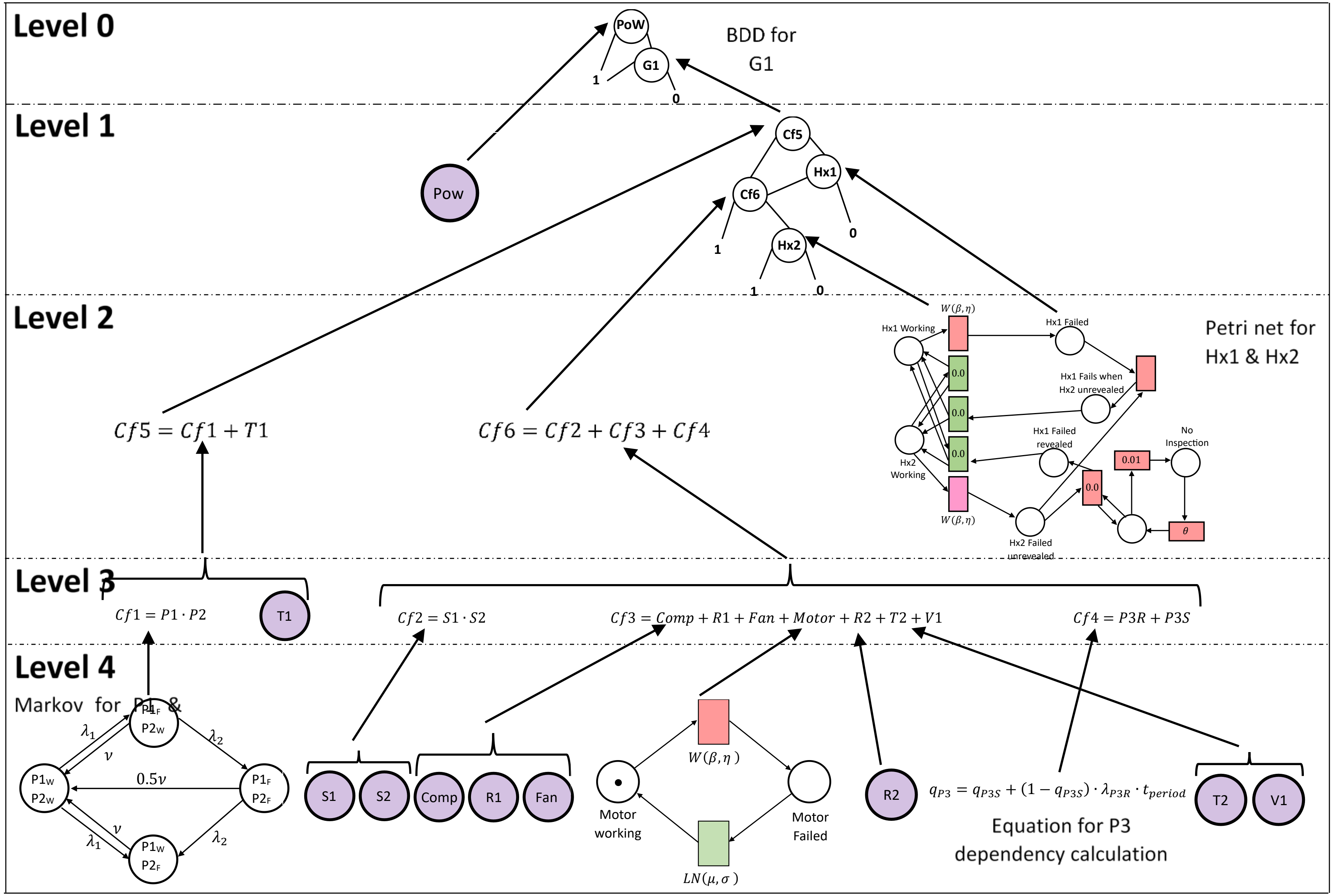
Pumps P1 & P2 – if one fails it puts increased load (and increases the failure rate) of the other

Heat Exchangers Hx1 & Hx2 - when one needs replacement – needs specialist equipment and both are replaced

Non-constant failure / repair rates

Pump P3 - two events P3S and P3R are clearly dependent

Structure of the Analysis

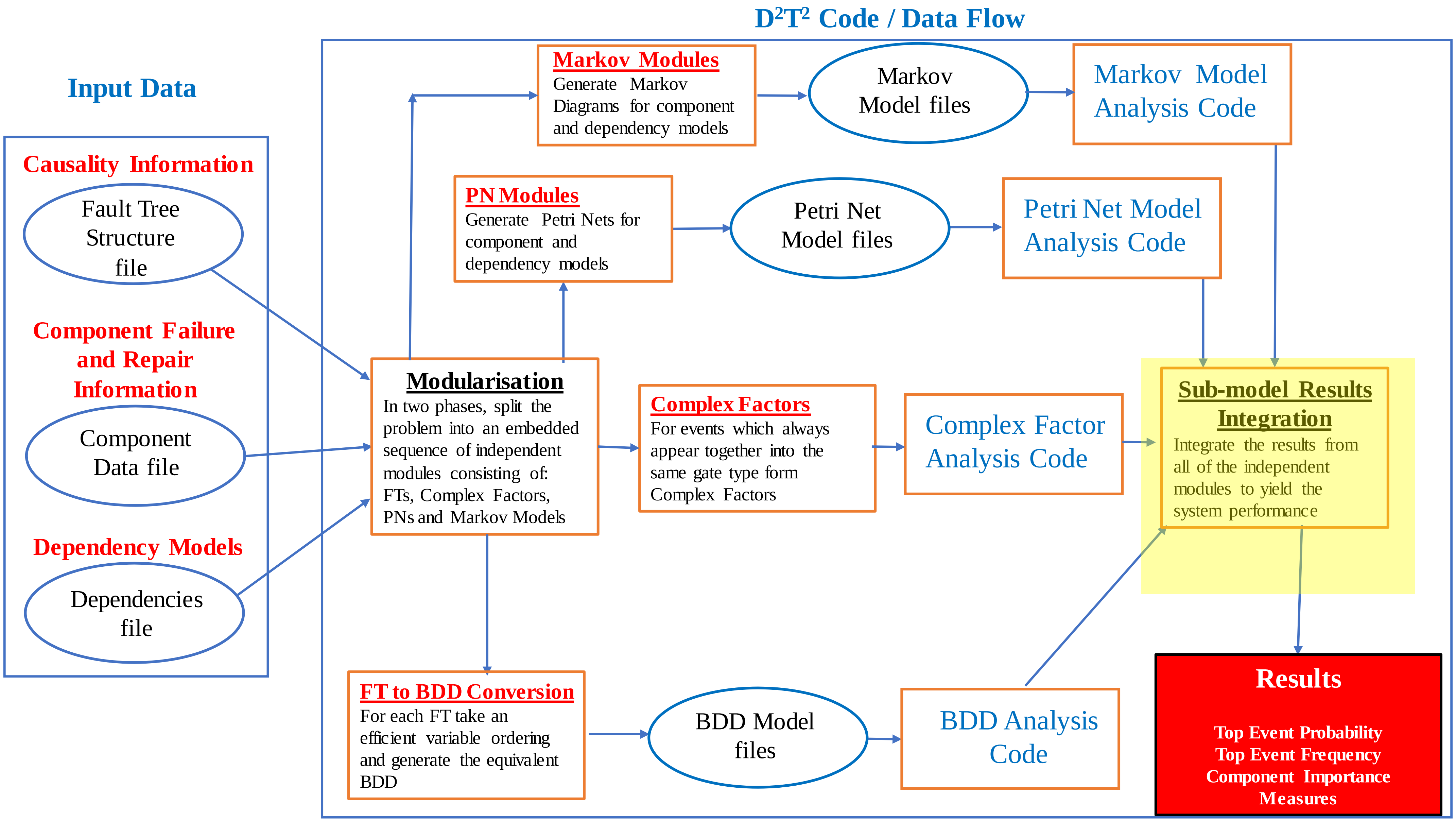


The function that represents system failure probability will be a function of probabilities taken from:

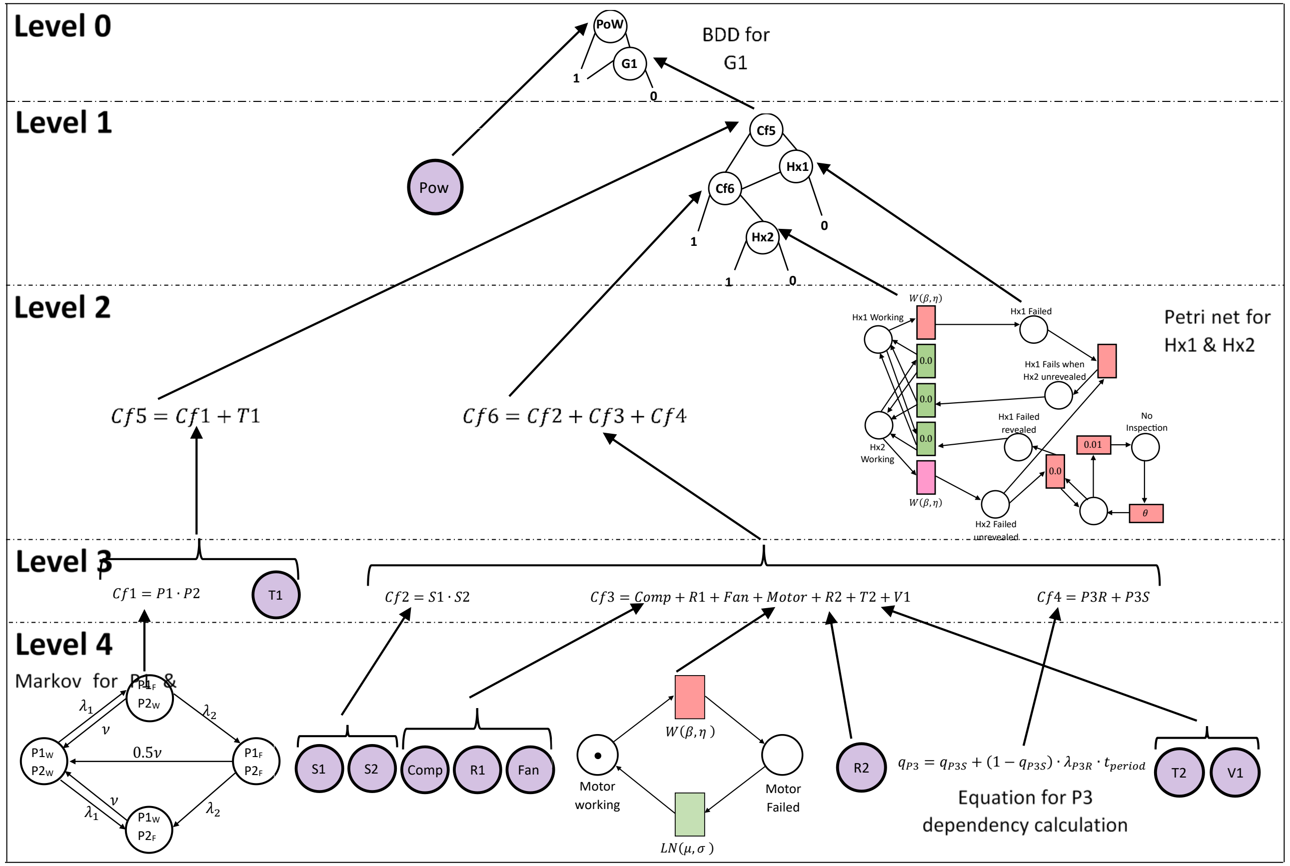
- Independent BDD modules, $BDD_j^I, j = 1, \ldots\ldots, N_1$,
- Dependent BDD modules, $BDD_j^D, j = 1, \ldots\ldots, N_2$,
- *Petri Net modules*, $PN_j \;, j = 1, \ldots\ldots, N_3$,
- Markov modules, $MKV_j \;, j = 1, \ldots\ldots, N_4$,
- Complex Factor modules, $Cfj, j = 1, \ldots\ldots, N_5$
- Components, $Cj, j = 1, \ldots N_6$

Top Event Probability Calculation

Basic Structure of the Code



Modularisation



$$Cf1 = P1.P2$$

$$Cf2 = S1.S2$$

$$Cf3 = Comp + R1 + Fan + Motor + R2 + T2 + V1$$

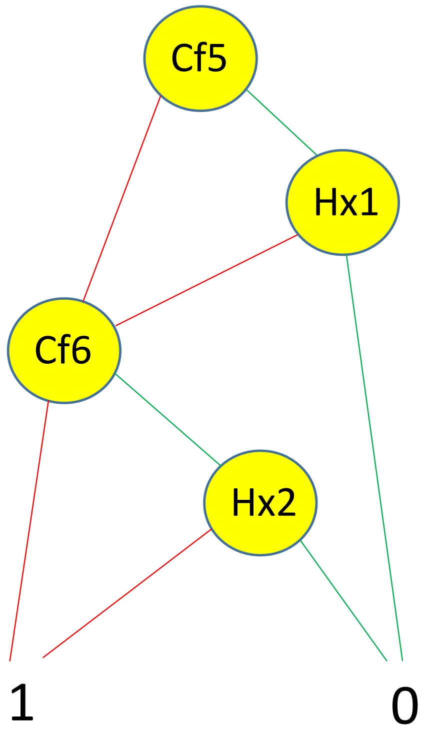
$$Cf4 = P3S + P3R$$

$$Cf5 = Cf1 + T1$$

$$Cf6 = Cf2 + Cf3 + Cf4$$

$Q_{Cf1} = 0.00170988$
$Q_{Cf2} = 0.034225$
$Q_{Cf3} = 0.144687275700137\,5$
$Q_{Cf4} = 0.1184$
$Q_{Cf5} = 0.0019494121410861265$
$Q_{Cf6} = 0.2717634478124872$

Integration



j	$path_j$	$Ipath_j$	$Dpath_j^1$
1	$Cf5_1, Cf6_1$	$Cf5_1, Cf6_1$	
2	$Cf5_1, Cf6_0, Hx2_1$	$Cf5_1, Cf6_0$	$Hx2_1$
3	$Cf5_0, Hx1_1, Cf6_1$	$Cf5_0, Cf6_1$	$Hx1_1$
4	$Cf5_0, Hx1_1, Cf6_0, Hx2_1$	$Cf5_0, Cf6_0$	$Hx1_1, Hx2_1$

$$Q_{G1} = \sum_{j=0}^{npath} \left[P(Ipath_j). \prod_{k=1}^{ndep} P(Dpath_j^k) \right]$$

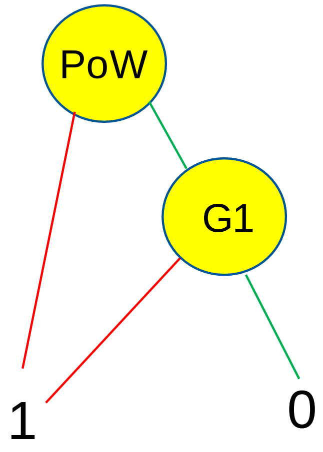
$$Q_{G1} = 0.00054898674$$

$$Q_{path1} = P(Cf5_1).\,P(Cf6_1) = 0.000529778965$$

$$Q_{path2} = P(Cf5_1).\,(1 - P(Cf6_1)).\,P(Hx2_1) = 1.920777884 \times 10^{-6}$$

$$Q_{path3} = (1 - P(Cf5_1)).\,P(Cf6_1).\,P(Hx1_1) = 0.0$$

$$Q_{path4} = (1 - P(Cf5_1)).\,(1 - P(Cf6_1)).\,P(Hx1_1, Hx2_1) = 0.0$$



$$Q_{path1} = P(PoW) = 0.000999$$

$$Q_{path2} = (1.0 - P(PoW))\,P(G1) = 0.0005484383$$

$$Q_{SYS} = 0.001547439304205123$$

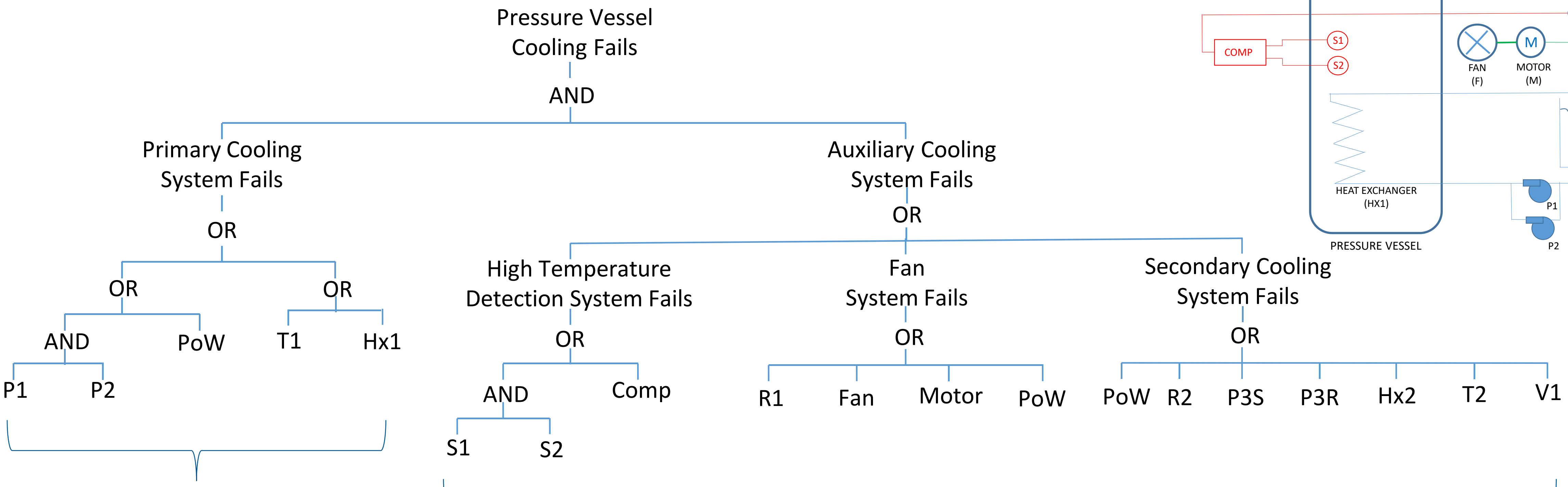
$Q_{Cf1} = 0.00170988$
$Q_{Cf2} = 0.034225$
$Q_{Cf3} = 0.1446872757001375$
$Q_{Cf4} = 0.1184$
$Q_{Cf5} = 0.0019494121410861265$
$Q_{Cf6} = 0.2717634478124872$
$Q_{G1} = 0.0005489867435093285$

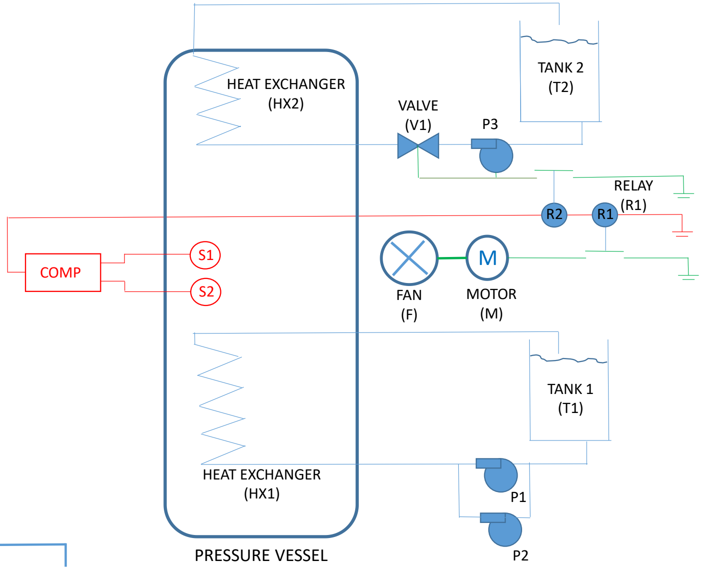
$\mathbf{Q_{sys} = 0.0015474393042051234}$

Top Event Frequency Calculation

Initiators / Enablers

Fault Tree Structure





Initiating events

Enabling events (other than PoW)

Results – Frequency Calculations

$Cf1 = P1.P2$ (Initiators)

$Cf2 = S1.S2$ (Enablers)

$Cf3 = Comp + R1 + Fan + Motor + R2 + T2 + V1$ (Enablers)

$Cf4 = P3S + P3R$ (Enablers)

$Cf5 = Cf1 + T1$ (Initiators)

$Cf6 = Cf2 + Cf3 + Cf4$ (Enablers)

$G1$

TOP

$Q_{Cf1} = 0.00170988$ $w_{Cf1} = 4.2747 \times 10^{-6}$

$Q_{Cf2} = 0.034225$

$Q_{Cf3} = 0.144687275700137$

$Q_{Cf4} = 0.1184$

$Q_{Cf5} = 0.00194941214108612$

$Q_{Cf6} = 0.2717634478124872$ $w_{Cf5} = 4.26534317 \times 10^{-11}$

$Q_{G1} = 0.0005489867435093$ $w_{G1} = 5.0115564890 \times 10^{-6}$

$w_{sys} = 0.000104851806008713$ / hour

University of Nottingham UK | CHINA | MALAYSIA

Minimal Cut Sets

PoW		
T1	Comp	
T1	R1	
T1	Fan	
T1	Motor	
T1	R2	
T1	T2	
T1	V1	
T1	P3	
T1	Hx2	
Hx1	Comp	
Hx1	R1	
Hx1	Fan	
Hx1	Motor	
Hx1	R2	
Hx1	T2	

Hx1	V1		
Hx1	P3		
Hx1	Hx2		
P1	P2	Comp	
P1	P2	R1	
P1	P2	Fan	
P1	P2	Motor	
P1	P2	R2	
P1	P2	T2	
P1	P2	V1	
P1	P2	P3	
T1	S1	S2	
P1	P2	Hx2	
Hx1	S1	S2	
P1	P2	S1	S2

1 min cut set of order 4
11 min cut set of order 3
18 min cut set of order 2
1 min cut set of order 1

Total Number of Minimal Cut Sets 31

Importance Measures

Top Event Probability

- Birnbaum’s Measure
- Criticality Measure
  Fussell-Vesely Measure
- Risk Achievement Worth
- Risk Reduction Worth

Top Event Frequency

- Barlow-Proschan Initiator Measure
- Barlow-Proschan Enabler Measure

Summary

- The Dynamic and Dependent Tree Theory (D^2T^2) approach has been presented
- The framework removes the need to assume:
  - Basics events are independent
  - Component failure times and repair times are governed by the exponential distribution
  - Simplistic maintenance processes
- This approach for fault tree analysis can be incorporated into event tree analysis

Thank you for your attention

Any Questions?

- Any comments on the methodology and the value of the ability to consider dependencies accurately.
- What do you look for when considering dependencies in Safety Cases?